

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

25. 8. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 8月18日

出 願 番 号  
Application Number: 特願2003-294056  
[ST. 10/C]: [JP2003-294056]

REC'D 15 OCT 2004	
WIPO	PCT

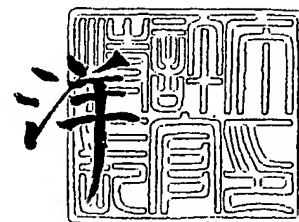
出 願 人  
Applicant(s): サイエンスパーク株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 9月30日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



【書類名】 特許願  
【整理番号】 PSP03002  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 13/10  
G06F 13/38

【発明者】  
【住所又は居所】 神奈川県座間市入谷4丁目3011番地の6 東建座間ハイツ2  
-509 サイエンスパーク株式会社内  
【氏名】 小路 幸市郎

【発明者】  
【住所又は居所】 神奈川県座間市入谷4丁目3011番地の6 東建座間ハイツ2  
-509 サイエンスパーク株式会社内  
【氏名】 野▲崎▼ 隆

【特許出願人】  
【識別番号】 501180263  
【氏名又は名称】 サイエンスパーク株式会社

【代理人】  
【識別番号】 100093687  
【弁理士】  
【氏名又は名称】 富崎 元成

【選任した代理人】  
【識別番号】 100106770  
【弁理士】  
【氏名又は名称】 岡城寺 貞夫

【選任した代理人】  
【識別番号】 100107951  
【弁理士】  
【氏名又は名称】 山田 勉

【手数料の表示】  
【予納台帳番号】 012911  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1

**【書類名】 特許請求の範囲****【請求項 1】**

データを記憶するデータ記憶手段と、  
認証用の識別データが登録されている識別データ記憶手段と、  
ユーザの認証情報を入力する入力手段と、  
前記入力手段からの入力データと、前記識別データ記憶手段に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段と、  
電子計算機と接続して前記データの送受信を行うインターフェース手段とを備え、  
前記認証の結果、前記入力データと前記識別データが一致するときに前記データへのアクセスを許可する電子データ管理装置において、  
制御プログラムを記憶するプログラム記憶手段を有し、  
前記認証手段によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になることを特徴とする電子データ管理装置。

**【請求項 2】**

請求項 1 において、  
前記認証手段による前記認証が完了した後、前記電子データ管理装置のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置の自動認識を開始することを特徴とする電子データ管理装置。

**【請求項 3】**

請求項 1 又は 2 において、  
前記データ記憶手段と前記プログラム記憶手段とをスイッチするスイッチ制御手段を有し、  
前記スイッチ制御手段は、前記プログラム記憶手段と接続されていて、前記ユーザ認証が行われ、前記制御プログラムが前記電子計算機にインストールされた後、前記データ記憶手段側にデータ読み取りを切り替えることを特徴とする電子データ管理装置。

**【請求項 4】**

請求項 1 ないし 3 から選択される 1 項において、  
前記電子計算機から前記データ記憶手段に書き込みすることが可能で、前記データを用いて前記電子計算機で操作した履歴又は前記電子計算機を操作した履歴が前記データ記憶手段に書き込まれることを特徴とする電子データ管理装置。

**【請求項 5】**

請求項 1 ないし 4 から選択される 1 項において、  
前記識別データは指紋データであり、  
前記入力手段から前記ユーザの指紋情報を入力し、  
前記認証手段では前記ユーザの指紋認証を行うことを特徴とする電子データ管理装置。

**【請求項 6】**

請求項 1 ないし 4 から選択される 1 項において、  
前記識別データは登録暗証番号であり、  
前記入力手段から暗証番号を入力し、  
前記認証手段では前記暗証番号と前記登録暗証番号と比較して前記ユーザの認証を行うことを特徴とする電子データ管理装置。

**【請求項 7】**

請求項 1 ないし 4 から選択される 1 項において、  
前記認証手段は錠と鍵を有し、  
前記鍵を持っている前記ユーザに前記データへのアクセスを許可する

ことを特徴とする電子データ管理装置。

【請求項 8】

登録された認証用情報を記憶する認証用情報領域と、  
ユーザの識別情報を入力する入力部と、  
前記認証用情報と、前記入力部から入力された前記入力情報とを比較して前記ユーザの認証を行うための認証機能を有する認証部と、  
データを記憶するデータ記憶領域と、  
制御プログラムを記憶するプログラム記憶領域と  
を有し、  
電子計算機と接続されると前記認証部によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域にアクセスする許可を与える電子データ管理装置において、  
前記認証が行われた後に前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用して作業を行うとき、前記作業の履歴を記憶するように前記電子計算機を動作させる

ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 9】

請求項 8 において、  
前記電子計算機との前記接続が切断されると、前記制御プログラムが前記電子計算機内に送信された前記データを削除する  
ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 10】

請求項 8 又は 9 において、  
前記制御プログラムが自動消滅する機能を有する  
ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 11】

請求項 8 ないし 10 から選択される 1 項において、  
前記制御プログラムは、  
前記電子計算機で前記データを複製、削除、編集、閲覧、読み込み、書き出しから選択される一以上の履歴、又は前記データを用いて作成したファイル、データの履歴を取得する履歴取得機能と、  
前記履歴を前記データ記憶領域に書き込みするデータ記録機能と、  
通信手段を利用して前記履歴を送信する送信機能と  
を有する  
ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 12】

請求項 11 において、  
前記履歴は、  
前記電子計算機のキーボードから入力された入力履歴、又はマウスを操作した操作履歴である  
ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 13】

請求項 8 ないし 12 から選択される 1 項において、  
前記制御プログラムが前記データを前記電子計算機内に特定アプリケーションで又は任意に複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の操作だけをできるように前記電子計算機のファイルシステムに制限をする  
ことを特徴とする電子データ管理装置用制御プログラム。

【請求項 14】

請求項 8 ないし 13 から選択される 1 項において、  
前記制御プログラムがカーネルモードで動作する

ことを特徴とする指紋認証電子データ管理装置用制御プログラム。

【請求項 1 5】

電子データ管理装置が、  
認証用情報を記憶する認証情報記憶部と、  
ユーザの認証情報を入力する入力部と、  
前記入力部からのデータを用いて前記ユーザの認証を行う認証部と、  
データを記憶するデータ記憶部と  
を有し、

電子計算機に接続されると前記認証部によって前記ユーザの前記認証が行われ、前記記憶部に登録されたデータと一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可する

データアクセス方法において、

前記電子データ管理装置が制御プログラムを格納するプログラム記憶部を有し、  
前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、  
前記電子計算機で前記データを利用する利用環境を確保する  
ことを特徴とするデータ管理方法。

【請求項 1 6】

請求項 1 5 において、

前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する制限である

ことを特徴とするデータ管理方法。

【請求項 1 7】

請求項 1 5 又は 1 6 において、

前記制御プログラムは、キーボードからの入力、マウス操作などの前記電子計算機を操作する履歴、又は前記データを用いて複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイルの履歴を残す機能を有する

ことを特徴とするデータ管理方法。

【請求項 1 8】

請求項 1 5 ないし 1 7 から選択される 1 項において、

前記電子データ管理装置と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルなどの内 1 つ以上を削除する

ことを特徴とするデータ管理方法。

【請求項 1 9】

請求項 1 5 ないし 1 8 から選択される 1 項において、

前記制御プログラムが自動消滅する機能を有する

ことを特徴とするデータ管理方法。

**【書類名】 明細書****【発明の名称】 電子データ管理装置、その制御プログラム及びデータ管理方法****【技術分野】****【0001】**

本発明は、ユーザのデータを格納し、管理する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。詳しくは、電子計算機に接続して使用する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。更に詳しくは、生体情報、暗証番号、鍵等を利用して個人認証を行い、メモリに格納されているデータへのアクセスを許可する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。

**【背景技術】****【0002】**

電子計算機にアクセスするときに、ユーザの認証を行っている。このユーザ認証には、ユーザ名とパスワードをキーボードから入力するパスワード式認証、人間の指紋、掌形、声紋、顔、虹彩等の生体情報を利用するバイオメトリクス認証がある。また、電子計算機と接続して利用する周辺装置を利用するときもユーザ認証を行うことができる。

**【0003】**

特に、外部記憶デバイスへアクセスするとき、セキュリティ面からは、ユーザ認証が重要である。従来から、電子計算機の本体、その周辺装置の電源、ケースなどに暗証番号又は鍵付きのロックを設けているものがある。その暗証番号を知っているユーザ又はその鍵を所持しているユーザのみが利用することができる。

**【0004】**

外部記憶デバイスで利用されている記憶メディアとしては、数多くの種類がある。代表的なものとしては、ハードディスク、MO、DVD-RAMがあり、ギガバイト以上の大容量のメディアである。また、コンパクトフラッシュ（登録商標）やスマートメディア（登録商標）、メモリスティック（登録商標）等のフラッシュメモリは数十から数ギガバイト容量の記憶メディアである。

**【0005】**

ユーザはこれらのメディアにデータを記録して別の場所で再生したり、作業を継続したりする他、必要に応じて他人にデータを渡すときも利用している。これらの外部記憶メディアを再生するデバイスがUSB（Universal Serial Bus）等のインターフェースで電子計算機に接続されて、記録データの送受信を行っている。例えば、マイクロソフト社（登録商標）のWindows Me（登録商標）、Windows 2000（登録商標）、WindowsXP（登録商標）の場合は、PnP機能を利用して電子計算機に接続されたデバイスを自動認識している。

**【0006】**

USBインターフェースで電子計算機にデバイスを接続すると、PnP機能が自動的にデバイスを認識して必要なドライバをインストールするか、又はドライバインストールの指示を画面に表示させて、ユーザはその指示に従ってドライバをインストールして、接続デバイスを利用できる環境を提供している。これにより、接続された外部記憶装置のデータを読み込んだり、外部記憶装置へデータを書き込んだりする。

**【0007】**

電子計算機を利用しようとするとき、マウスの指紋認証部によって指紋認証を行うことができる。例えば、電子計算機に接続されているマウスに指紋認証機能を持たせたものとしては、特許文献1の「個人認証用マウス及びそのシステム」に開示している。その他の例としては、記憶メディアに指紋認証情報を設けている例がある。

**【0008】**

例えば、特許文献2の「可搬性記録媒体および可搬性記録媒体の使用方法」においては、CD-RWにアプリケーションソフトウェア、ユーザ認証プログラム、指紋認証エンジンと、利用者の指紋情報等を格納して、指紋照合によるユーザ認証、認証後のアプリケーションソフトウェアの利用を提供している。

## 【0009】

また、特許文献3の「電子データ管理装置、方法及び記録媒体」には、電子帳簿システムに関し、磁気カードに登録された取引情報が入力されて電子帳簿ファイルの修正を行うものである。このとき、磁気カードに登録された指紋情報と、電子帳簿システムに接続されている指紋認証装置から入力された指紋情報と、電子帳簿システム内のデータベースに登録されている指紋情報がすべて一致するときのみ電子帳簿ファイルの修正を許可している。

【特許文献1】特開2001-125734 「個人認証用マウス及びそのシステム」

【特許文献2】特開2001-229017 「可搬性記録媒体および可搬性記録媒体の使用法」

【特許文献3】特開2000-353204 「電子データ管理装置、方法及び記録媒体」

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0010】

フラッシュメディアなどによってデータを運び、別の電子計算機で読み込んで使用する場合、又は他人に渡して利用してもらう場合がある。しかし、ユーザにとっては、一般的にデータは重要なものであり、これらのデータをそのまま第三者に渡すことは元より、電子計算機にも残したくない。例えば、印刷業者に頼んで印刷を行うとき、ユーザは印刷データをフレキシブルディスクやCD-ROMなどの媒体に入れて提供することが一般的である。印刷業者がこれらのデータを利用して印刷した後は、媒体を戻しても、データが業者の電子計算機内に残ることになる。これはユーザにとってセキュリティの面では好ましくない。

## 【0011】

本発明は上述のような技術背景のもとになされたものであり、下記の目的を達成する。

本発明の目的は、電子計算機と接続されると自動的にインストールされて電子計算機内のデータの制御を行うことができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。

本発明の他の目的は、電子計算機から切断されると電子計算機に送信された、または電子計算機内に加工されたデータ、作成されたファイル等を消去することができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。

## 【0012】

本発明の更に他の目的は、電子計算機から切断されると自ら消滅することができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。

本発明の更に他の目的は、個人認証機能を有する電子データ管理装置、その制御プログラム、及びデータ管理方法を提供する。

## 【課題を解決するための手段】

## 【0013】

本発明は、前記目的を達成するため、次の手段を採用する。

本発明の第1の発明の電子データ管理装置は、データを記憶するデータ記憶手段と、認証用の識別データが登録されている識別データ記憶手段と、ユーザの認証情報を入力する入力手段と、前記入力手段からの入力データと、前記識別データ記憶手段に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段と、電子計算機と接続して前記データの送受信を行うインターフェース手段と制御プログラムを記憶するプログラム記憶手段を有する。

## 【0014】

電子データ管理装置は、前記認証の結果、前記入力データと前記識別データが一致する

ときに前記データへのアクセスを許可し、前記認証手段によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になると良い。

【0015】

また、前記認証手段による前記認証が完了した後、前記電子データ管理装置のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置の自動認識を開始すると良い。

更に、前記データ記憶手段と前記プログラム記憶手段とをスイッチするスイッチ制御手段を有し、前記スイッチ制御手段は、前記プログラム記憶手段と接続されていて、前記ユーザ認証が行われ、前記制御プログラムが前記電子計算機にインストールされた後、前記データ記憶手段に切り替えをすると良い。

【0016】

また更に、前記電子計算機から前記データ記憶手段に書き込みすることが可能で、前記データを用いて前記電子計算機で操作した履歴又は記電子計算機を操作した履歴が書き込まれると良い。前記識別データは指紋データで、前記入力手段から前記ユーザの指紋情報を入力し、前記認証手段では前記ユーザの指紋認証を行うと良い。

【0017】

更に、前記識別データは登録暗証番号で、前記入力手段から暗証番号を入力し、前記認証手段では前記暗証番号と前記登録暗証番号と比較して前記ユーザの認証を行うと良い。更に、前記認証手段は錠と鍵を有し、前記鍵を持っている前記ユーザに前記データへのアクセスを許可すると良い。

【0018】

本発明の第2の発明の電子データ管理装置用制御プログラムは、電子データ管理装置内に記録されている制御プログラムであり、電子データ管理装置は、制御プログラムを記憶するプログラム記憶領域を有し、前記認証が行われた後に前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用して作業を行うとき、前記作業の履歴を記憶するように前記電子計算機を動作させるプログラムである。

【0019】

また、電子データ管理装置は、登録された認証用情報を記憶する認証用情報領域と、ユーザの識別情報を入力する入力部と、前記認証用情報と、前記入力部から入力された前記入力情報とを比較して前記ユーザの認証を行う認証機能を有する認証部と、データを記憶するデータ記憶領域とを有し、電子計算機と接続されると前記認証部によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域にアクセスする許可を与えると良い。

【0020】

また、電子データ管理装置用制御プログラムは、前記電子計算機との前記接続が切断されると、前記制御プログラムが前記電子計算機内に送信された前記データを削除すると良い。更に、前記制御プログラムが自動消滅する機能を有すると良い。

更に、前記電子計算機で前記データを複製、削除、編集、閲覧、読み込み、書き出しした履歴、又は前記データを用いて作成したファイル、データの履歴を取得する履歴取得機能と、前記履歴を前記データ記憶領域に書き込みするデータ記録機能と、通信手段を利用して前記履歴を送信する送信機能とを有すると良い。

【0021】

また更に、前記履歴は、前記電子計算機のキーボードから入力された入力履歴、又はマウスを操作した操作履歴であると良い。

前記制御プログラムが前記データを前記電子計算機内に特定アプリケーションで又は任意に複製、削除、編集、閲覧、読み込み、書き出しする操作のいずれか1以上の操作だけができるように前記電子計算機のファイルシステムに制限をすると良い。電子データ管理装置用制御プログラムが前記制御プログラムがカーネルモードで動作すると良い。

【0022】



本発明の第3の発明のデータ管理方法は、認証用情報を記憶する認証情報記憶部と、ユーザの認証情報を入力する入力部と、前記入力部からのデータを用いて前記ユーザの認証を行う認証部と、データを記憶するデータ記憶部とを有する電子計算機に接続され、前記認証部によって前記ユーザの前記認証が行われ、前記記憶部に登録されたデータと一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可するデータ管理方法であって、前記電子データ管理装置が制御プログラムを格納するプログラム記憶部を有し、前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用する利用環境を確保する。

#### 【0023】

また、前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する制限であると良い。

更に、前記制御プログラムは、キーボードからの入力、マウス操作などの前記電子計算機を操作する履歴、又は前記データを用いて複製、削除、編集、閲覧、読み込み、書き出しする操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイルの履歴を残す機能を有すると良い。

#### 【0024】

また更に、前記電子データ管理装置と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルなどの内1つ以上を削除すると良い。更に、前記制御プログラムが自動消滅する機能を有すると良い。

#### 【発明の効果】

#### 【0025】

本発明によると、次の効果が奏される。

本発明は、電子計算機にインストールされてユーザデータの管理を行う制御プログラムを格納した電子データ管理装置を提供することによって、ユーザデータの正確な利用、セキュリティを向上させることが可能になった。

#### 【0026】

本発明は、電子計算機でユーザデータを利用して作業を行っても作業後データが残ることがないデータ管理を図ることができる。

本発明は、認証機能付きの電子データ管理装置を提供することによって、特定のユーザのみがアクセスできるようになった。

#### 【発明を実施するための最良の形態】

#### 【0027】

##### 〔実施の形態1〕

図1には、本発明の実施の形態1の概要を図示している。図1には、電子データ管理装置1の構成例の概要を図示している。電子データ管理装置1は、筐体2、筐体2の一面に設けた指紋情報入力部3、筐体2と接続されているコネクタ4から構成されている。図2には、筐体2に格納される基板5の構成の概要を図示している。

#### 【0028】

基板5の上には、第1メモリ6、第2メモリ7、USB (Universal Serial Bus) コントローラ9、中央演算装置 (CPU、Central Processing Unit) 8等が配置されている。第1メモリ6は、ユーザのデータ及びファイル等のユーザデータを格納するためのメモリである。第2メモリ7は、制御プログラムを格納するためのメモリである。USBコントローラ9は、コネクタ4を介して電子計算機 (図示せず) との送受信を制御するためのプログラムである。CPU8は、電子データ管理装置1全体を制御するための中央演算処理装置である。

#### 【0029】

電子データ管理装置1が電子計算機と接続され、制御プログラムが電子計算機にインストールされると、スイッチ10が第2メモリ7から第1メモリ6へと切り替わり、ユーザデータの送受信が可能になる。また、基板5には、認証用データベース11、認証モジュ

ール12が配置されている。認証モジュール12は指紋情報入力部3と連動してユーザの認証を行うためのものである。認証用データベース11は、電子データ管理装置1を使用できるユーザの指紋情報等の識別データを格納したデータベースのためのメモリである。

#### 【0030】

図3は、電子データ管理装置1へこの識別データを記録する手順を示すフローチャートである。図3に図示したように、電子データ管理装置1を利用する前に、電子データ管理装置1へユーザデータを書き込み、ユーザの指紋情報を登録する。電子データ管理装置1へユーザデータを書き込みするための専用のアプリケーションプログラムがインストールされている電子計算機に、電子データ管理装置1を接続して、その専用のアプリケーションプログラムによってユーザのデータを電子データ管理装置1の第1メモリ6に書き込む(ステップ1)。

#### 【0031】

そして、電子データ管理装置1を利用するユーザの指紋情報などの識別情報を認証用データベース11に登録する(ステップ2)。識別情報の登録が完了すると、電子計算機から電子データ管理装置1を抜き取って持ち出しが可能になる(ステップ3)。これらのユーザデータおよび、ユーザの指紋情報などの識別情報は、専用のファイルシステムを用いて行われても良い。

#### 【0032】

図4は、電子データ管理装置1を利用するときの全体の流れを図示したフローチャートである。電子データ管理装置1を電子計算機にUSBコネクタを用いて接続する(ステップ10)。電子データ管理装置1がユーザの指紋認証を行う(ステップ11)。ユーザの指紋認証は、指紋情報入力部3からの指紋情報データを用いて認証モジュール12が行う。

#### 【0033】

このとき、認証モジュール12はユーザの指紋情報データを予め登録した識別データと比較して、「正当なユーザであるか?」を判定する(ステップ12)。ユーザの指紋情報データが認証用データベース11に格納されている識別データと一致しない場合は、「利用許可がないユーザ」と判定されて電子データ管理装置1を利用することができない(ステップ13)。

#### 【0034】

ユーザの指紋情報データが認証用データベース11に格納されているデータと一致する場合は、「正当なユーザである」と判定されて次の処理に移る。USBコネクタ4のPnP機能が許可され開始する(ステップ14)。第2メモリ7に格納されている制御プログラムが電子計算機にインストールされる(ステップ15)。制御プログラムは電子計算機にインストールされて、ユーザがユーザデータを用いて作業できる環境を確保する。

#### 【0035】

制御プログラムのインストールが正常に行われたかの判定を行う(ステップ16)。電子計算機、その上で動作するOSの設定によっては、外部からプログラム等のインストールができない場合がある。この場合は、制御プログラムのインストールが行われないので、電子データ管理装置1をこの電子計算機で利用することができない(ステップ17)。

#### 【0036】

制御プログラムが正常にインストールされると、スイッチ10が第1メモリ6への切り替えを行い、第1メモリ6を利用可能になる(ステップ18)。第1メモリ6には、ユーザデータが保存されており、電子計算機へ転送することが可能になる。また、電子計算機上のアプリケーションプログラムから第1メモリ6へアクセスしユーザデータを呼び出すなどの作業を行うことができるようになる(ステップ19)。

#### 【0037】

また、同時に電子計算機にインストールされている制御プログラムが、履歴情報などのデータを第1メモリ6に書き込むことができるようになる。履歴情報には、ユーザデータを利用した履歴、ユーザデータを利用して作成したファイルの履歴、キーボード入力、マ

ウス操作等の電子計算機を操作した履歴、電子計算機から周辺デバイス、通信回線を利用して行われたやりとりの履歴などが含まれても良い。USBコネクタ4が切断されると（ステップ20）、電子計算機にインストールされている制御プログラムが電子計算機内のユーザデータを削除する（ステップ21）。

#### 【0038】

このとき、ユーザデータを利用し、加工して作ったデータ、ファイルの削除を行っても良い。そして、電子計算機にインストールされた制御プログラムが自動消滅する（ステップ22）。このように、電子データ管理装置1の利用するとき、電子計算機上にはユーザデータが残ることがない。

#### 【0039】

電子データ管理装置1を利用するためには、予め利用できるユーザの識別情報を認証用データベース11に登録しておく。電子データ管理装置1のデータは通常のインターフェースでアクセスできない状態になっている。電子データ管理装置1へのアクセスがロックされていて、ユーザ認証が正常に行われて、利用許可のあるユーザのみが電子データ管理装置1を利用することができる。そのとき、電子データ管理装置1のアクセスロックが解除されて、電子計算機へのアクセス、コネクタの接続が行われる。

#### 【0040】

##### 〔実施の形態2〕

図5は、本発明の実施の形態2の概要を図示したフローチャートである。ユーザデータ、ユーザの指紋情報などの識別データが登録された電子データ管理装置1を使用する電子計算機に接続する（ステップ100）。電子データ管理装置1がユーザの認証を指紋情報入力部3からの指紋情報データを用いて認証モジュール12が行なう（ステップ101）。ユーザの指紋識別データを予め登録した指紋情報と比較して正当なユーザであるかを判定する（ステップ102）。

#### 【0041】

ユーザの指紋情報が認証用データベース11に格納されているデータと一致しない場合は、利用許可がないユーザと判定され再度ユーザ認証が行われる（ステップ103）。これは、電子データ管理装置1が切断されるか、ユーザ認証が成功するまで続く。ユーザの指紋情報データが認証用データベース11に格納されている識別データと一致した場合は正当なユーザであると判定され次の処理に移る。

#### 【0042】

電子データ管理装置1をアンロックにし（ステップ104）、PNP機能が有効になり、PNP機能が開始する（ステップ105）。PNP機能を利用して、電子計算機が電子データ管理装置1を自動認識する。電子計算機が電子データ管理装置1を自動認識し終わると、通常の外付けメモリと同様にアクセスできるようになる（ステップ106）。電子データ管理装置1のUSBコネクタを切断すると（ステップ107）、電子計算機との一連のデータの送受信が終了する。この実施の形態では、電子計算機に転送され、書き込まれたデータに関しては特別に制限を設けていない。電子データ管理装置1を持ち出してそれにアクセスできるユーザの認証を行ってからアンロックし、アクセス許可を行っている。

#### 【0043】

##### 〔実施の形態3〕

図6には、本発明の実施の形態3の概要を図示している。本実施の形態3は、配布元と使用者からなるシステムに関し、使用者は配布元のデータを用いて作業を行い、その結果を配布元に報告するものである。また、配布元は提供するデータを特定の制限範囲だけに使用できる環境も提供している。

#### 【0044】

図6には、電子データ管理装置1（以下、ハードウェアという）を提供する配布元、それを使用する使用者とのやりとりの流れを図示している。配布元は、ファイルシステムの機能を拡張した拡張ファイルシステムを提供する（ステップ200）。

## 【0045】

拡張ファイルシステムは、使用者が利用したアプリケーションプログラムの履歴、データの読み取り・編集・書き込みの履歴、ファイルの読み込み・書き込み・複製・作成・削除などの履歴を取る機能を有する。また、電子計算機のファイルシステムが提供する機能を制限する機能も有する。更に、ユーザのキーボード入力の履歴、マウスのクリック等のマウスを操作する履歴を取る機能も有する。

## 【0046】

使用者は、この拡張ファイルシステムを導入する（ステップ201）。配布元は、ハードウェアを提供する（ステップ202）。それと同時に、ハードウェアと連携して動作するユーティリティの提供も可能である。使用者は、使用するアプリケーションプログラムを配布元に申請し（ステップ203）、配布元はアプリケーションプログラムに対するハードウェア固有のファイルとデータを使用者に提供する（ステップ204）。

## 【0047】

使用者は、これを受け取ってハードウェアを電子計算機に接続する（ステップ205）。ハードウェアが電子計算機に接続されると、拡張ファイルシステムがハードウェアを認識し、制御モードに入る（ステップ206）。制御モードに関する情報は、配布元が提供したハードウェア固有のファイルに含まれている。

## 【0048】

使用者が、配布元のデータを利用して作業を行う。これらの作業の履歴が記録される（ステップ207）。ファイル使用履歴は、ハードウェアに記録される（ステップ208）。作業が終了すると、「作業の完了」の通知を配布元に送信する（ステップ209）。配布元はこの「作業の完了」通知を受け取る（ステップ214）。

## 【0049】

そして、履歴データを配布元に送信する（ステップ210）。配布元は、履歴データを受信し（ステップ215）、受信したら応答する（ステップ216）。拡張ファイルシステムがこの応答を受信したら、複製ファイル、作業ファイル、そのデータ等を削除する（ステップ211）。そして、制限モードを解除し、通常のファイルシステムのモードに入る（ステップ212）。

## 【0050】

これらの一連の作業が終了すると、使用者はハードウェアを配布元に返す（ステップ213）。配布元は、履歴データを受信してから、使用者が履歴データを解析して（ステップ217）、提供ファイル、データを正確に使用したかを把握することができる。また、返却されてハードウェア内に保存されている履歴データを解析して把握することも可能である（ステップ218）。

## 【0051】

使用者から配布元への履歴データなどの送信は専用通信回線、インターネット、公衆通信網などの通信網によって行われる。使用者と配布元は、通信網は通信網で接続されていない場合は、ハードウェアにそれらの履歴が保存されてハードウェアを返却することによって行われる。

## 【0052】

## 〔実施の形態4〕

図7には、本実施の形態4の概要を図示している。本実施の形態4では制御プログラムが電子計算機にインストールされて、ユーザが使用するアプリケーションプログラムを登録できるようになっている。

## 【0053】

電子データ管理装置1を電子計算機と接続してユーザ認証が行われる（ステップ301）。ユーザ認証が完了すると、電子データ管理装置1のアクセスロックが解除されて電子計算機とやり取りできるようになり、PnP機能が有効になる。よって、電子データ管理装置1が電子計算機に認識されて、電子データ管理装置1のドライバのインストールが開始される（ステップ302）。電子データ管理装置1のドライバのインストール終了後は

、制御プログラムのインストールが開始される (303)

【0054】

このとき、ユーザからアプリケーションプログラムの登録をすることが可能である (ステップ304)。ユーザはアプリケーションプログラムの登録をしない場合は、制御プログラムのインストールが続けて行われる (ステップ306)。ユーザがアプリケーションプログラムの登録を行う場合は、登録するアプリケーションプログラムを選択し、そのファイル名、パス、ディレクトリなどを指定、選択して登録を行う。 (ステップ305)。

【0055】

アプリケーションプログラムの登録が終わると、制御プログラムのインストールが続けて行われる (ステップ306)。制御プログラムが正常にインストールされたかを確認して電子データ管理装置1の使用が可能になる (ステップ307、308、309)。

【0056】

また、上述のようにユーザが制御プログラムをインストールするときアプリケーションプログラムを登録し、その使用履歴を取得し、登録されたアプリケーションプログラムの使用範囲を制限することが可能である。アプリケーションプログラムの他に特定のデータ、ファイルを登録しても良い。データ、ファイルを登録すると、実施の形態1のようにデータ、ファイルの使用履歴を追跡して把握することが可能になる。ユーザは、制御プログラムを使用中でも、アプリケーションプログラム、データ、ファイルの登録、登録の取り消しすることも可能である。

【0057】

〔実施の形態5〕

図8には、本発明の実施の形態5の概要を図示している。本実施の形態5では、電子データ管理装置1が切断されても制御プログラムを継続して使用可能なものを提供している。USBコネクタが切断される (ステップ350)。そのとき、アンインストールを開始するかを確認する (ステップ351)。アンインストールしない場合は、電子データ管理装置1を継続して使用できる (ステップ356)。

【0058】

アンインストールを開始するときは、今まで使用したデータを削除するかを確認し (ステップ352)、電子計算機内のデータを削除する (ステップ353)。そして、制御プログラム自身を削除するかを確認する (ステップ354)。データと制御プログラムを削除しない場合は、それぞれ続けて電子データ管理装置1を使用する (ステップ356)。ただし、制御プログラムの削除を行った場合は、継続して電子データ管理装置1を使用することができない (ステップ355)。

【0059】

〔実施の形態6〕

本実施の形態6は電子データ管理装置1の他の実施の形態である。図9には、本実施の形態6の概要を図示している。電子データ管理装置20は、筐体2、筐体2の一辺に設けた押しボタン式のキー21、そしてコネクタ4から構成されている。

【0060】

電子データ管理装置20は、実施の形態1から5の電子データ管理装置1とはユーザ認証には暗証番号を利用している点が異なる。その他の機能は、前述した電子データ管理装置1と同様であり、詳しい説明は省略する。違っている部分の説明だけを行う。ユーザは、電子データ管理装置20のロックを解除するために、その一辺に設けている押しボタン式のキー21から暗証番号を入力する。

【0061】

暗証番号を入力するときに、その入力開始、入力終了を識別するために「#」、「\*」などの決められた記号キーを暗証番号入力の前後に押しても良い。押しボタン式のキー21は0～9までの数字、一部の記号のボタンを有しているが、電子データ管理装置20の大きさ、用途に合わせてボタンの数を増減しても良い。

【0062】

電子データ管理装置 20 の内部構造は図 2 と同様であり、ユーザ認証は認証モジュール 12 が行い、その認証のためにはあらかじめ登録された暗証番号が認証用データベース 11 に記憶されている。

#### 【0063】

この電子データ管理装置 20 を利用するまでの手順は、図 10 のフローチャートに示している。専用のアプリケーションプログラムでユーザデータを電子データ管理装置 20 の第 1 メモリ 6 に書き込み、暗証番号を認証用データベース 11 に登録する（ステップ 401、402）。よって、電子データ管理装置 20 が利用可能になる。

#### 【0064】

##### 〔実施の形態 7〕

本実施の形態 7 は電子データ管理装置 1 の他の実施の形態である。図 11 には、本実施の形態 7 の概要を図示している。錠 32 と鍵 31 の組を用いたユーザ認証を行う電子データ管理装置 30 の概要を図示している。電子データ管理装置 30 は、筐体 2、筐体 2 の一辺に設けた錠 32、そしてコネクタ 4 から構成されている。錠 32 を開閉するための鍵 31 が 1 組になって付属する。電子データ管理装置 30 の内部構造は図 2 と同様であり、ユーザ認証は認証モジュール 12 が行う。ユーザ認証は、錠 32 の開閉によって行われるので、認証用データベース 11 が不要である。

#### 【0065】

実施の形態 1 から 5 の電子データ管理装置 1 とはユーザ認証に錠 32 と鍵 31 の組を利用している点異なる。その他の機能は、前述の電子データ管理装置 1 と同様であり、詳しい説明は省略する。異なる部分の説明だけを行う。

#### 【0066】

ユーザは、電子データ管理装置 30 のロックを解除するために、その一辺に設けている錠 32 に矢印 33 の方向で示すように鍵 31 を差し込んで錠 32 のロックを解除する。この情報を、認証モジュール 12 が察知し、電子データ管理装置 30 のアクセスロックを解除し、電子データ管理装置 30 へのアクセスが可能になる。

#### 【0067】

本発明の実施の形態は、これまでに記述したような実施の形態 1 から 7 のみに適用され利用されるものではなく、同様な効果が得られ場どのような形式・形態でも利用しても良い。

#### 【産業上の利用可能性】

#### 【0068】

本発明は、ユーザのファイルやデータなどを携帯可能なメモリ装置に記録して搬送して使用することが可能であり、セキュリティが必要な業界で利用すると良い。特に、営業または経理データ等でユーザデータやファイルなどの秘密情報の提供が必要とされる印刷業界、販売店で利用されることが望ましい。また、ペーパーレス処理を行うための機関、顧客へのファイル提供などに利用されても良い。音楽配信、映像配信、電子出版などの電子コンテンツ配信サービスを行うとき、被受信者を特定し、被受信者のメモリに電子コンテンツを書き込んで提供するときに利用されても良い。

#### 【図面の簡単な説明】

#### 【0069】

【図 1】図 1 は、電子データ管理装置 1 の構成例の概要を図示している図面である。

【図 2】図 2 は、電子データ管理装置 1 の基板 5 の構成例を図示している概念図である。

【図 3】図 3 は、電子データ管理装置 1 を利用する前の準備の手順を図示しているフローチャートである。

【図 4】図 4 は、電子データ管理装置 1 を利用する全体の流れを図示したフローチャートである。

【図 5】図 5 は、本発明の実施の形態 2 の概要を図示したフローチャートである。

【図 6】図 6 は、本発明の実施の形態 3 の概要を図示したフローチャートである。

【図 7】図 7 は、本発明の実施の形態 4 の概要を図示したフローチャートである。

【図 8】図 8 は、本発明の実施の形態 5 の概要を図示したフローチャートである。

【図 9】図 9 は、暗証番号を用いて認証を行う実施の形態 6 の概要を図示した図である。

【図 10】図 10 は、電子データ管理装置 20 の利用する準備の手順を図しているフローチャートである。

【図 11】図 11 は、鍵を用いて認証を行う実施の形態 7 の概要を図示した図である。

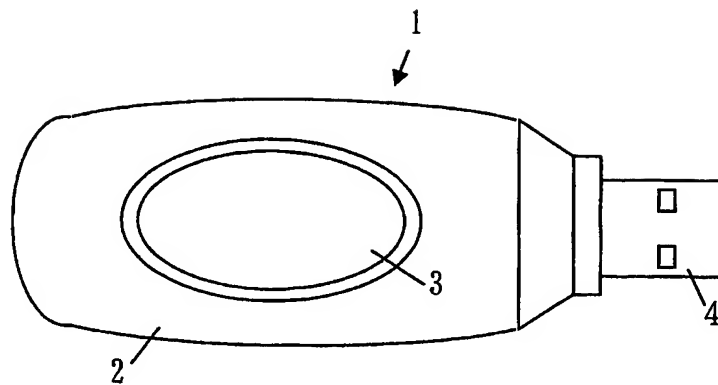
【符号の説明】

【0070】

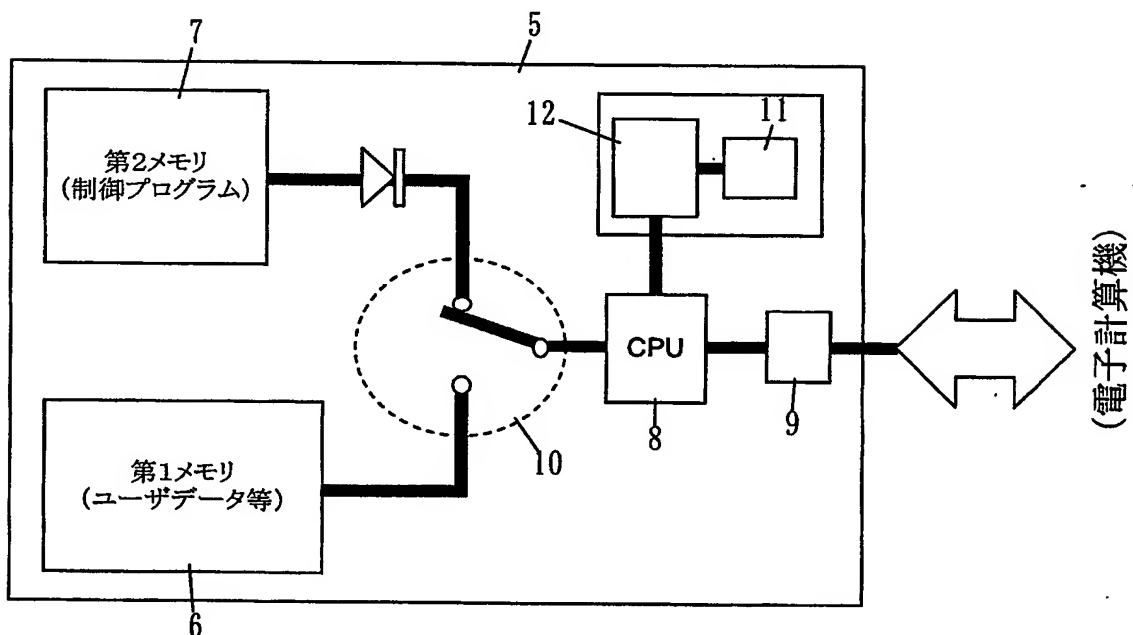
- 1…電子データ管理装置
- 2…筐体
- 3…指紋認証部
- 4…USBコネクタ
- 5…基板
- 6…第 1 メモリ
- 7…第 2 メモリ
- 8…CPU
- 9…バスコントローラ
- 10…スイッチ
- 11…指紋認証用データベース
- 12…指紋認証部
- 20…電子データ管理装置
- 21…押しボタン式入力部
- 30…電子データ管理装置
- 31…鍵
- 32…錠

【書類名】 図面

【図1】

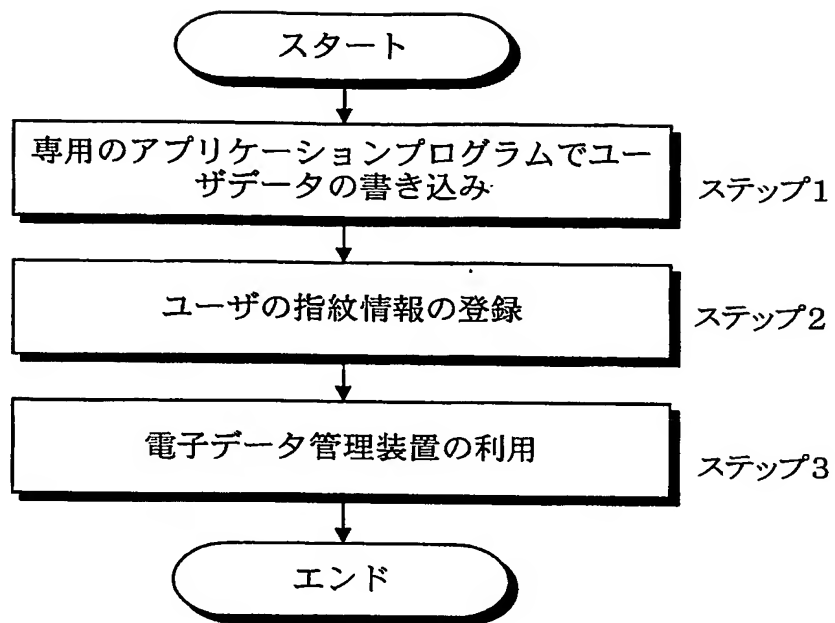


【図2】

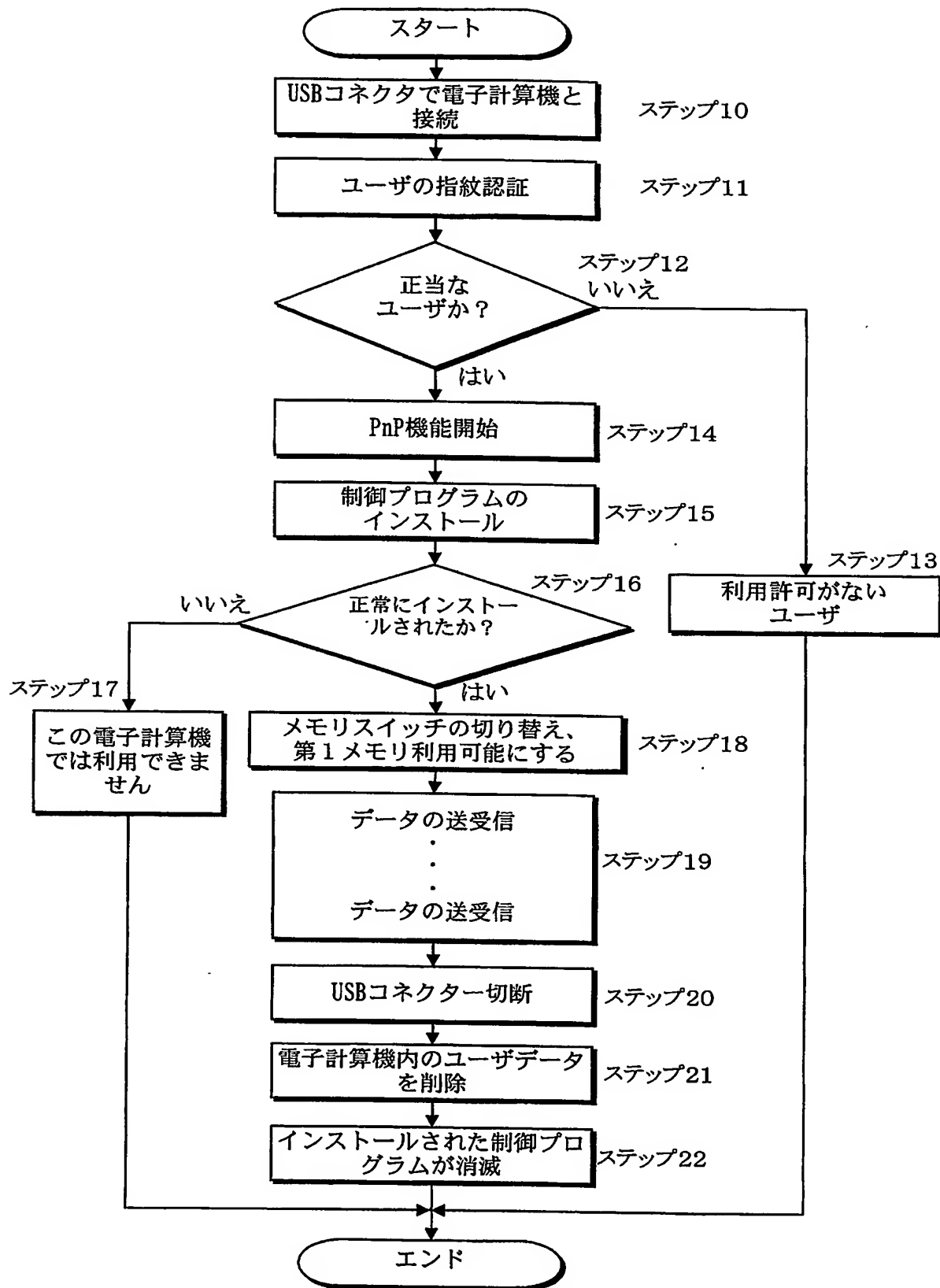




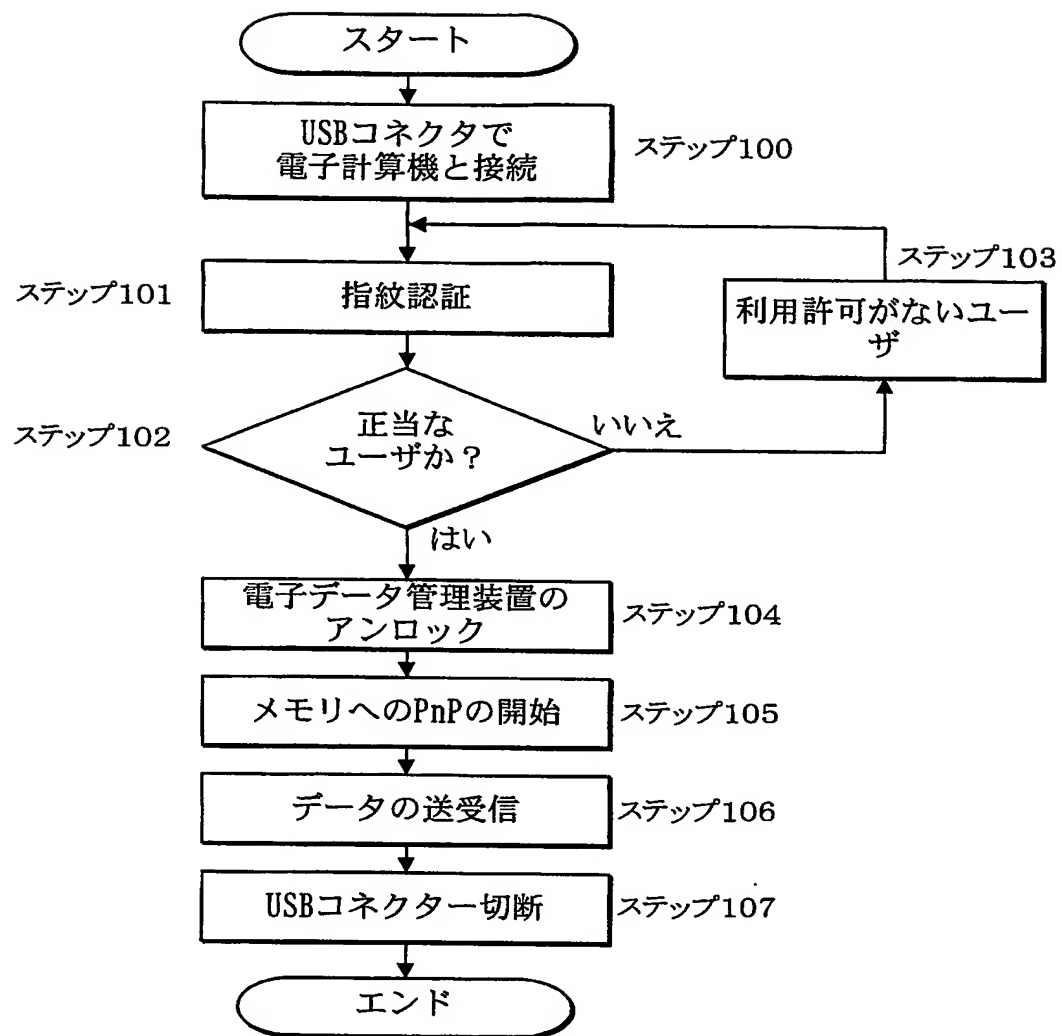
【図 3】



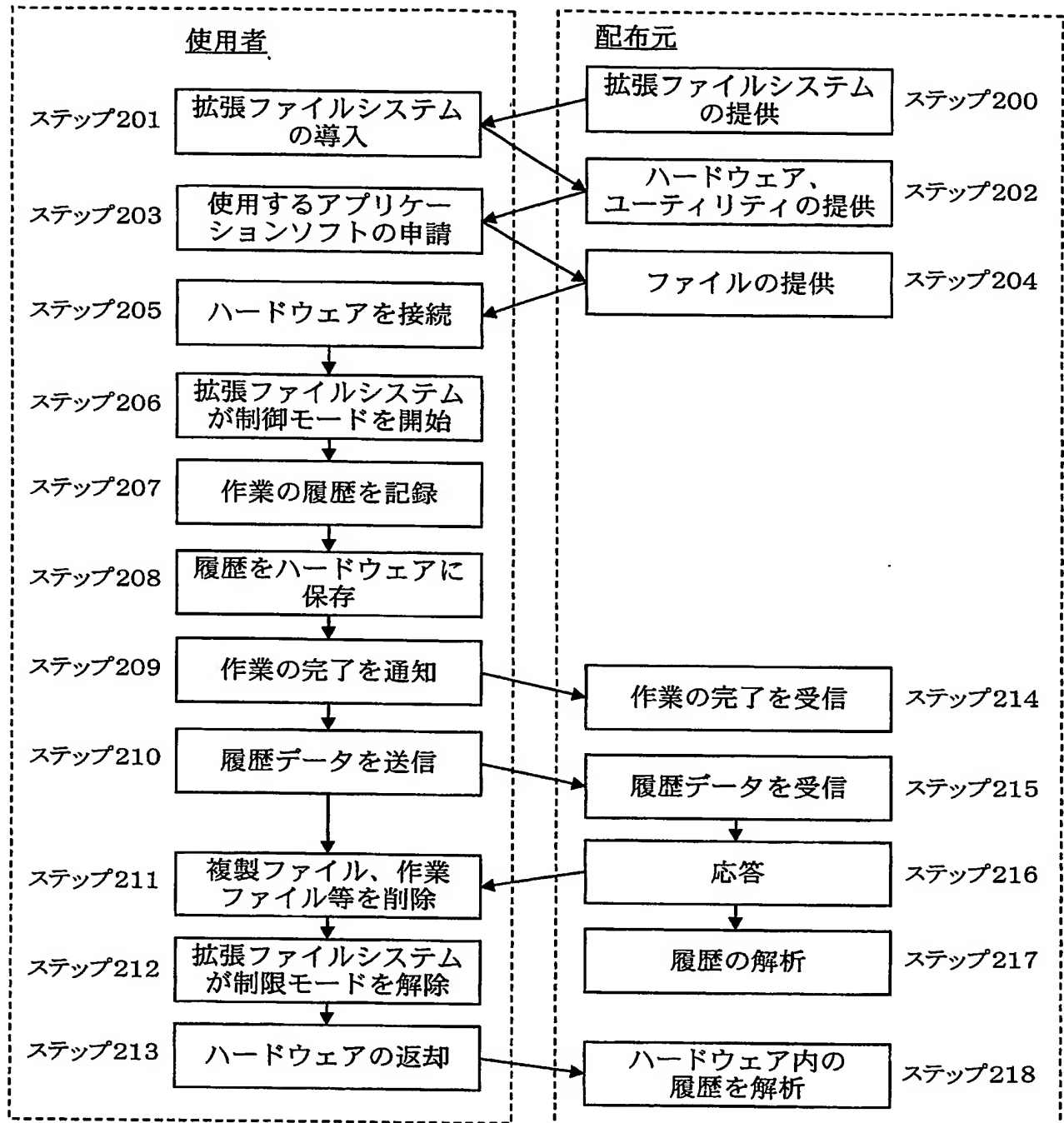
【図 4】



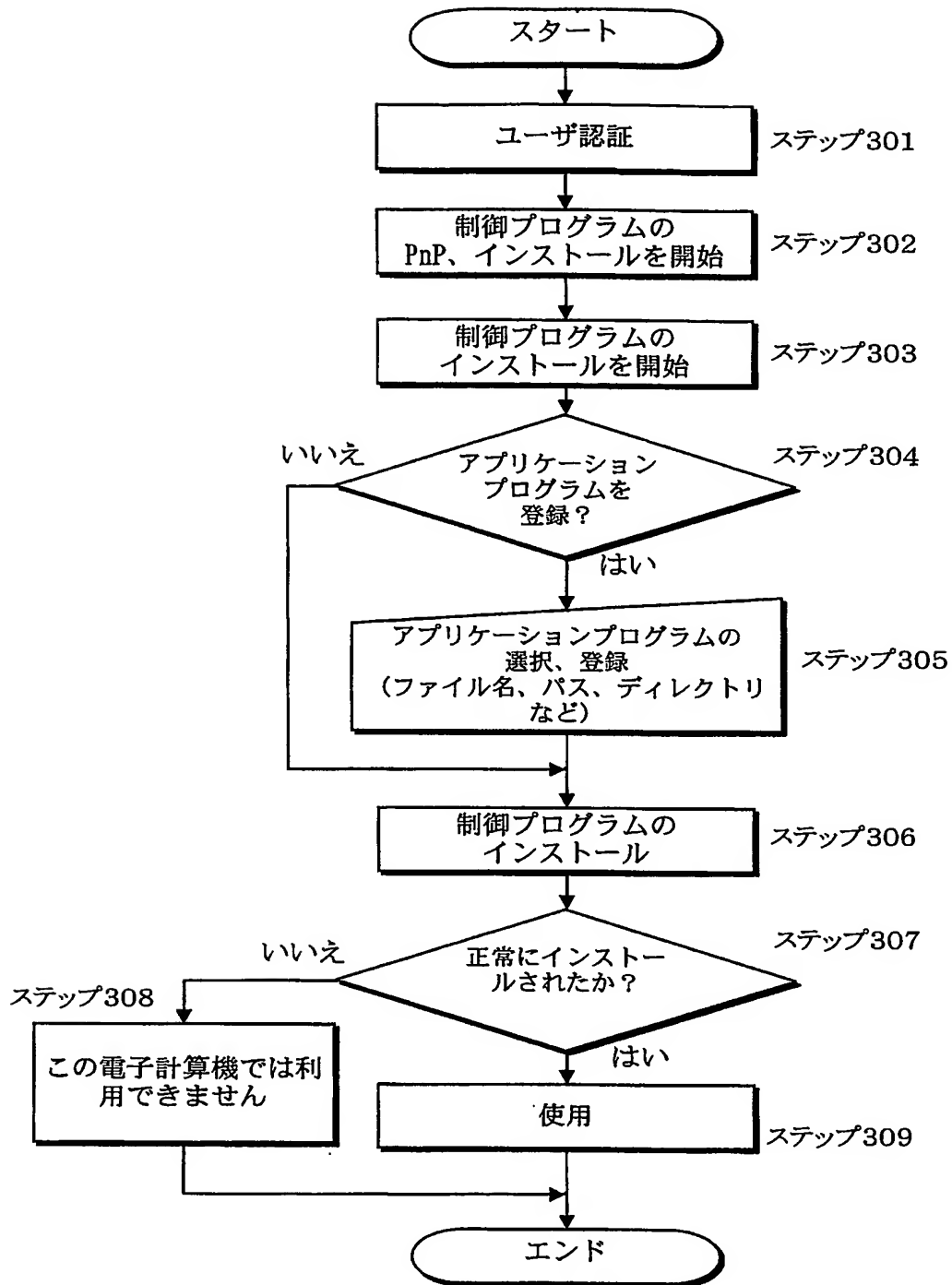
【図 5】



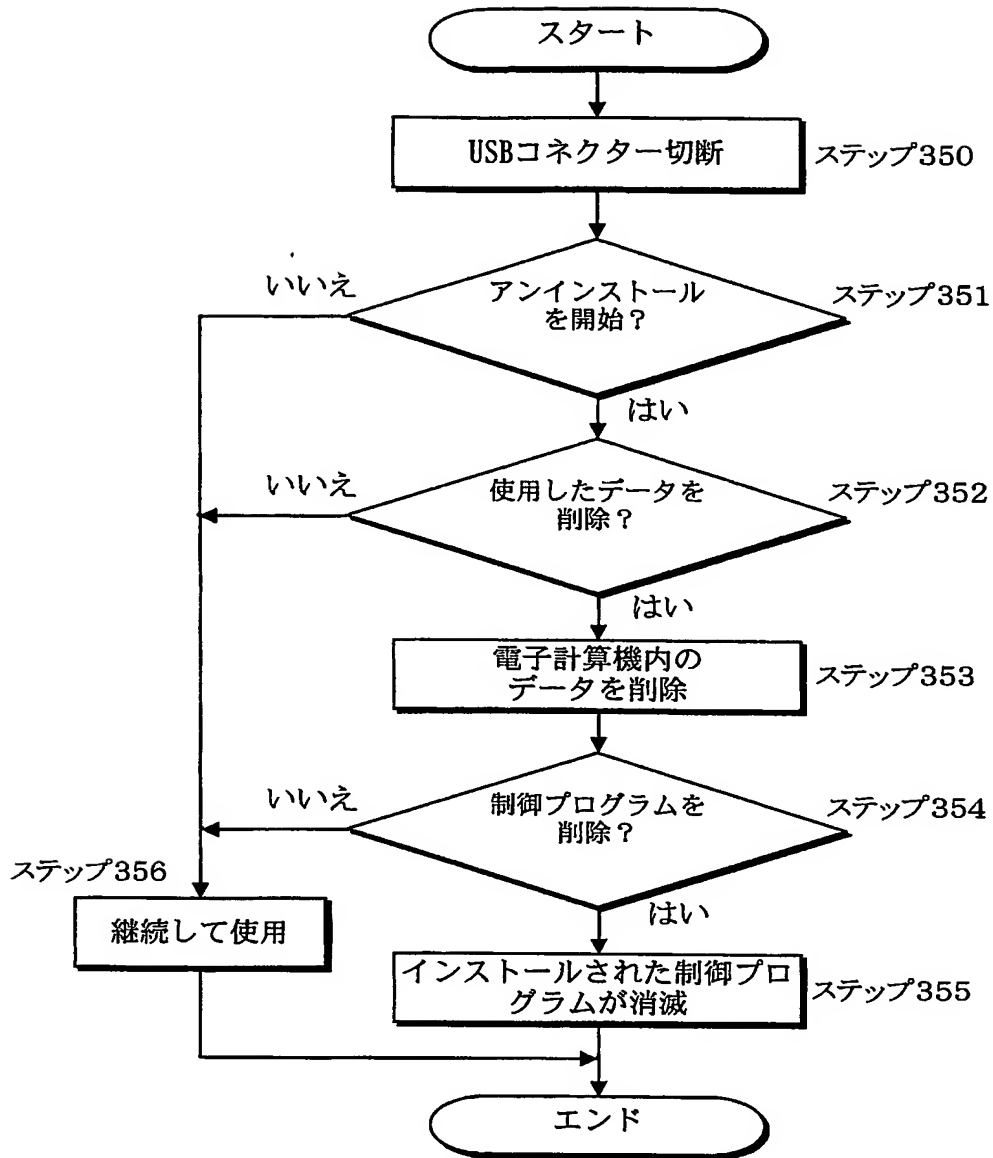
【図 6】



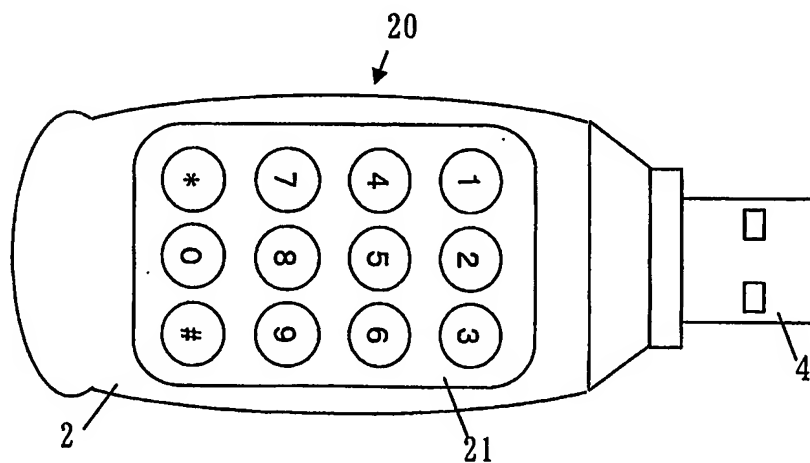
【図7】



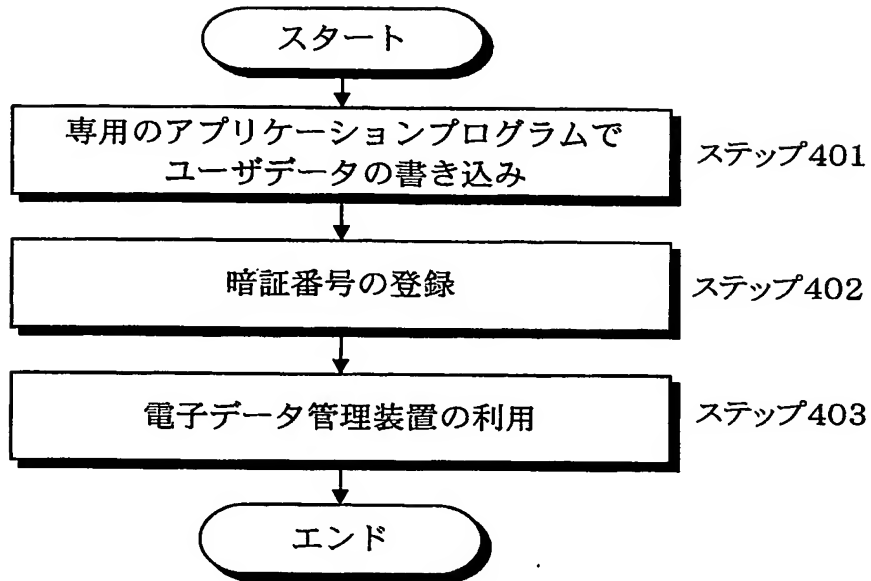
【図 8】



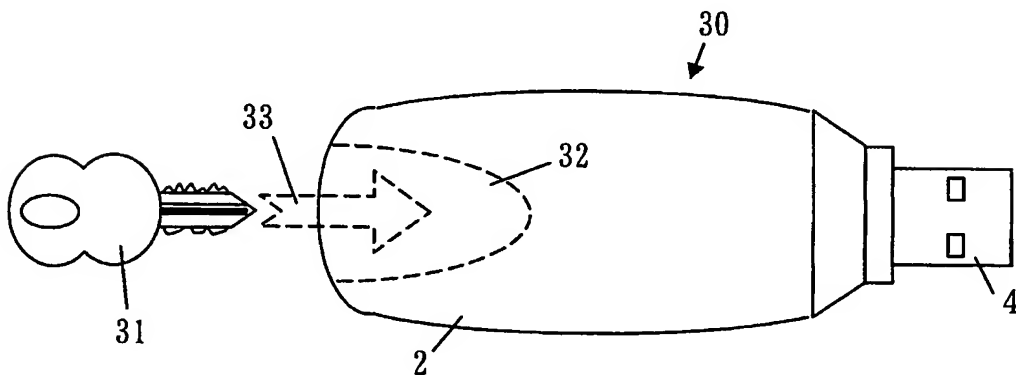
【図 9】



【図 10】



【図 11】



## 【書類名】要約書

## 【要約】

【課題】電子計算機と接続されると自動的にインストールされて電子計算機内のデータの制御を行うことができる制御プログラムを格納した電子データ管理装置を提供する

【解決手段】電子データ管理装置 1 は、ユーザデータを記憶する第 1 メモリ 6 と、識別データが登録されている認証用データベース 11 と、ユーザの認証情報を入力する入力部 3 と、入力部 3 からの入力データと、認証用データベース 11 の登録された識別データとを比較してユーザの認証を行う認証モジュール 12 と、電子計算機と接続して前記データの送受信を行う USB コネクタ 4、制御プログラムを記憶する第 2 メモリ 7 を備える。ユーザ認証後、制御プログラムが電子計算機にインストールされ、スイッチ 10 が第 2 メモリ 7 から第 1 メモリ 6 へと切り替えて、電子計算機からユーザデータを読み出しすることが可能になる。

【選択図】 図 1



認定・付加情報

特許出願の番号	特願 2 0 0 3 - 2 9 4 0 5 6
受付番号	5 0 3 0 1 3 5 1 9 7 4
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 8 月 1 9 日

< 認定情報・付加情報 >

【提出日】	平成15年 8月18日
-------	-------------

特願 2 0 0 3 - 2 9 4 0 5 6

出 願 人 履 歴 情 報

識別番号 [ 5 0 1 1 8 0 2 6 3 ]

1. 変更年月日	2 0 0 1 年 5 月 7 日
[変更理由]	新規登録
住 所	神奈川県座間市入谷 4 丁目 3 0 1 1 番地の 6 東建座間ハイッ
	2 - 5 0 9
氏 名	サイエンスパーク株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**